Getting Started in A Cybersecurity Career

David Wright

Director of Academic Technology and Curriculum Innovation

University of Dayton

University *of* Dayton
Center for
Cybersecurity &
Data Intelligence

OHIO CYBER
RANGE INSTITUTE

Overview

Cybersecurity is swiftly emerging as a critical facet of all professions, necessitating that employees in all roles familiarize themselves with cybersecurity best practices. Moreover, an array of fantastic job opportunities in cybersecurity have swiftly cemented their place as indispensable in this new field. This paper explores how individuals can explore whether cybersecurity might be a suitable career path for them, and how they can get started.

About the Author

David Wright is the Director of Academic Technology and Curriculum Innovation and an Associate Professor of Biology at the University of Dayton. His responsibilities include the management of academic technologies in the classroom, and several technology platforms for learning, teaching and faculty productivity. He is closely associated with faculty development and coordinates many professional development opportunities for faculty. David works closely with the university administration to make best use of technology resources for enhancing learning. David also teaches undergraduate biology classes at the University of Dayton. He has worked on several contracts for NASA that involved the creation of software used in the manned space program. David earned a Ph.D. in Anatomy from the University of Iowa in 1989, and completed his postdoctoral training at the University of Wisconsin.

University of Dayton
Center for Cybersecurity and Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at **go.udayton.edu/cybersecurity**

Getting Started in a Cybersecurity Career

David J. Wright
Director of Academic Technology and Curriculum Innovation
University of Dayton

Introduction

Cybersecurity is swiftly emerging as a critical facet of all professions, necessitating all employees, irrespective of their roles, familiarize themselves with cybersecurity best practices.[1] Moreover, there's an array of fantastic job opportunities specializing in cybersecurity that have swiftly cemented their place as indispensable in this new field.[2] [3] So, how can an individual explore this profession? How can they ascertain if this is a suitable career path for them? And how can they get started?

Is Cybersecurity Right for You?

Although media companies tend to sensationalize prominent hacking incidents, such news stories may be one of the first ways we realize the importance of securing data and building a secure cyber infrastructure. Perhaps these stories pique your interest and you subsequently want to learn more. It's also quite conceivable that you may be a target of a cyberattack and consequently develop an interest based on personal experience.

Whether you are a student in high school or a workforce professional, it can help to consider what soft skills you have that align with the cybersecurity profession. Here are some traits that can indicate someone may be well-suited for this field:

- *Strong sense of personal ethics:* Cybersecurity is rooted in trust and "doing the right thing."
- *Passion for security:* A genuine interest in the field and a passion for ensuring the security of systems and data is key for success.
- *Technical knowledge:* A strong background or interest in computer science, programming and networking can be highly valuable.
- *Curiosity and problem-solving:* Identify and solve complex problems in real-time, within diverse environments and often under pressure.
- *Attention to detail:* Meticulous in their work, as even small errors can have significant consequences.
- *Life-long learner:* Cybersecurity is a rapidly evolving field, and professionals must be able to adapt to new technologies, threats and solutions.
- *Communication skills:* Cybersecurity professionals often need to explain technical concepts to non-technical stakeholders and work in teams to defend against cyberattacks.

If you possess all or some of these skills, a cybersecurity career may be a good fit for you.[4]

[1] https://udayton.edu/cybersecurity/resources/index.php
[2] https://www.futureoftech.org/cybersecurity/
[3] Miller, A. (2022). Cybersecurity career guide. Manning Publications Co.
[4] https://www.cyberinternacademy.com/10-ways-to-know-if-cybersecurity-is-right-for-you/

More details of what is expected of cybersecurity professionals can be found in the NICE Framework – a comprehensive review of the skills and knowledge expected of employees in job roles related to cybersecurity.[5] The details in this resource from the National Initiative for Cybersecurity Education may be overwhelming, but generally these components are baked into the various educational programs you can participate in to train and become certified to work in cybersecurity positions. NIST provides a summary of this framework on their website.[6]

NICE also provides a great web resource with general information about cybersecurity jobs, expectations and resources for preparing for a career in this exciting IT profession.[7]

To encourage greater diversity within the workforce, NICE publishes information about numerous national programs and resources that ensure minority and underprivileged individuals are attracted to the field of cybersecurity.[8]

Are Cybersecurity Jobs Available?

Although cybersecurity is one of the newest fields of the information technology industry it is also one of the most in-demand by employers. The growth is fueled by the desperate need to protect enterprise computing environments while individual hackers and state-sponsored hacking efforts have created unprecedented risks. This has created an unusual "vacuum" where employer demand is outstripping supply of potential employees, whether these are drawn from recent graduates or from existing workers that decide to change jobs.

Nationally, over 600,000 cybersecurity job openings were posted in the past year. There are sufficient potential workers to fill only 69% of these openings.[9]

What are Some Specific Cybersecurity Jobs?

The following are the most common cybersecurity jobs, as reported by CyberSeek, 2023[10]:

- Cybersecurity Analyst
- Software Developer
- Penetration & Vulnerability Tester
- Cybersecurity Consultant
- Network Engineer
- Cybersecurity Manager
- Systems Engineer
- Senior Software Developer
- Systems Administrator

CyberSeek provides an interactive website that details the many cybersecurity-related careers along with the entry points.[11] Don't forget to scroll the interactive web page as you select each job title on this website to view more details – such as job descriptions.

[5] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice
[6] https://www.nist.gov/system/files/documents/2023/06/05/NICE%20Framework%20%28NIST%20SP%20800-181%29_one-pager_508Compliant.pdf
[7] https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-awareness-week/discovering-cybersecurity
[8] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/diversity-inclusion
[9] https://www.cyberseek.org/heatmap.html
[10] https://www.cyberseek.org/pathway.html
[11] https://www.cyberseek.org/pathway.html

Additional career pathway tools can be found on the NICE website[12] and the US Department of Homeland Security CISA website[13]. The Bureau of Labor Statistics from the US Department of Labor also provides basic job descriptions and salary information.[14]

An increasing number of non-IT occupations are tasked with duties that relate strongly to cybersecurity. For example: 1) lawyers and other members of the legal profession may need to be versed in cybersecurity practices when dealing with cyber-related criminal cases; 2) human resource staff would need to manage the data accessibility scope of employees; 3) public policy analysts would need to shape the regulation of data safety and management for state and local government agencies; and 4) technical writers would be tasked to write communiques to a non-technical audience about issues that originate in the technical world of cybersecurity. There are many more examples, and we can anticipate this broadening of the scope of cybersecurity to grow in the future.[15]

Getting Started

Early exposure to cybersecurity can come to students in schools and colleges or existing employees through participation in informal clubs and events. Competitions, such as hackathons, provide a great opportunity for developing a taste of the world of cybersecurity even if participating as an observer. Some games are designed to align with the NICE framework.[16] Find information about such events through local organizations and their various social media channels. Many events are coordinated to occur during a week in October as part of an annual Cybersecurity Career Week.[17]

Education

Pursuing a degree in computer science, information technology, or a related field can provide a strong foundation for a career in cybersecurity. Many universities and colleges now offer specific programs and degrees in cybersecurity, as shown in Cyberseek's interactive map.[18] For those parts of the country with the highest workforce demands, many educational institutions are connected through regional coordinating centers including ATE Centers[19], and RAMP Programs[20].

When reviewing different programs, a potential student would do well to look for the use of hands-on experiential learning opportunities embedded within the curriculum. For example, the use of cyber ranges is a powerful way for students to exercise their knowledge in a safe environment.[21] Many programs also leverage the use of apprenticeships and cooperative educational opportunities.[22]

Institutions of higher education can seek and obtain a type of accreditation from the NSA to document the alignment of curriculum and scholarship with national standards of excellence.[23] [24] When searching for an educational program, look for these National

[12] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/career-pathways

[13] https://niccs.cisa.gov/sites/default/files/documents/pdf/career%20profiles5.pdf?trackDocs=career%20profiles5.pdf

[14] https://www.bls.gov/ooh/computer-and-information-technology/home.htm

[15] https://hacktales.com.ng/2022/05/17/non-technical-cybersecurity-roles/

[16] https://static1.squarespace.com/static/5e13a4b584a68c775e362068/t/5f3ec0067388003a3d3c6252/1597947910523/NCL-NICE6+w+icons.pdf

[17] https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week

[18] https://www.cyberseek.org/training.html

[19] https://www.nist.gov/system/files/documents/2017/08/18/ate-one-pager_071116.pdf

[20] https://www.nist.gov/system/files/documents/2017/08/18/ramps_one_pager_032017.pdf8u_tpo.pdf

[21] https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

[22] https://www.nist.gov/system/files/documents/2018/01/09/nice_apprenticeship_one_pager_oct_31_2017.pdf

[23] https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[24] https://www.nist.gov/system/files/documents/2022/05/23/nice_cae_print_11_6_2017.pdf

Centers of Academic Excellence in Cybersecurity designations – namely CAE-CD, CAE-CO and CAE-R.[25]

Platforms like Coursera, Udemy, and edX offer a wide range of standalone cybersecurity courses that can help you develop specific skills and knowledge in the field. As higher education adapts to the use of micro-credentials, it is likely that in the future such standalone courses could be "stacked" to build a custom-built certificate or badge.

Popular certifications in the industry include CompTIA Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP). Such professional training is shown to lead to employee skills development and salary increases.[26]

Transition from an existing career may require the completion of a smaller set of courses to supplement an existing undergraduate or graduate degree. Typically, these courses are packaged as a certificate or other micro-credential, and many can include hands-on work experience.

Cybersecurity as a Vocation

Cybersecurity professionals are hired because of skills they possess that others in an organization may lack. But there are many human dimensions that define cybersecurity as a vocation and not simply a job. For example, becoming established in cybersecurity allows a person to grow and mature their commitment to privacy, ethics and collaborative engagement with diverse colleagues. Many of these dimensions are embedded to some extent in training or educational programs, but frequently personal reflection and mentorship can help shape a person's growth even when a career pathway is not very clear.[27] Bolstering a résumé with professional skill development is another way to continue this vocational journey, long after completing secondary or tertiary education. You may often hear of the phrase "life-long learning", and this truly applies to anyone seeking successful employment in cybersecurity.

Cybersecurity Over the Horizon

A key attribute of anyone in the IT industry is comfort with looking to the future. To most end-users, technology innovations can seem like magic (an addictive type of magic), but as IT professionals we must rationally plan for an uncertain future with rapidly evolving tools and methods. In joining the ranks of cybersecurity professionals, a person must develop an ability to look over the horizon. For example, artificial intelligence is clearly going to be a growing element of the cybersecurity threat environment – but it is also a powerful tool that can provide new defenses. The landscape could have other dramatic upheavals – such as the nature of the data that we protect. For example, widely-distributed sensors using IoT devices will flood the networks with important and sensitive data unlike anything we have seen before, or non-traditional data such as personal genomic sequences will be necessary for every single person. Perhaps in the distant future even uploaded dreams will be considered a type of data needing protection.

Cybersecurity is clearly going to continue to be an exciting part of the future IT experience and it will be important to consider the changing role of professionals working in this field.

[25] https://www.caecommunity.org/

[26] https://www.nist.gov/system/files/documents/2018/07/24/nice_value_of_certifications_7.19.18.pdf

[27] Oltsik, J., & Alexander, C. (2016). The Cyber Profession at Risk: Take Control of Your Cybersecurity Career Life Cycle. ISSA Journal, 14(10), 14–15.